COMMUNICATIONS
SECURITY
ESTABLISHMENT
COMMISSIONER

Annual Report

2006-2007

Canada

Office of the Communications Security
Establishment Commissioner
P.O. Box 1984
Station "B"
Ottawa, Ontario
K1P 5R5

Tel.: (613) 992-3044
Fax: (613) 992-4096
Website: http://csec-ccst.gc.ca

© Minister of Public Works and
Government Services Canada 2007
ISBN 978-0-662-69804-3
Cat. No. D95-2007

Communications Security
Establishment Commissioner

The Honourable Charles D. Gonthier, Q.C.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Charles D. Gonthier, c.r.

May 2007

Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Sir:

Pursuant to subsection 273.63 (3) of the *National Defence Act*, I am pleased to submit to you my 2006–2007 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,

Charles Gonthier

Charles D. Gonthier

P.O. Box/C.P. 1984, Station "B"/Succursale « B »
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

2007-03951/

TABLE OF CONTENTS

Introduction /1

The Review Environment /2
- Legal interpretations /2
- Legislation lagging behind technological advances /4
- Three-year review of the *Anti-Terrorism Act* /4
- Senate Special Committee recommendations /5
- House of Commons Subcommittee recommendations /7
- The O'Connor Commission of Inquiry /8

The Year in Review /10
- Independent reviews of OCSEC /10
- Workplan /10
- Reviews undertaken of CSE /11

2006-2007 Review Highlights /12
- Review of CSE's foreign intelligence collection in support of the RCMP /12
  - Background /12
  - Methodology /12
  - Findings /13
- Review of information technology security activities at a government department /14
  - Background /14
  - Methodology /15
  - Findings /15
- Review of the roles of CSE's client relations officers and the Operational Policy Section in the release of personal information /16
  - Background /16
  - Methodology /17
  - Findings /17

2006-2007 Review Highlights *(Continued)*

- Review of CSE signals intelligence collection activities conducted under ministerial authorizations /18
  - Background /18
  - Methodology /19
  - Findings /19
- Overview of 2006-2007 findings /19
- Reviews underway/future reporting /20
- Complaints about CSE activities /20
- Duties under the *Security of Information Act* /20

The Commissioner's Office /21

Looking to the Future /22

- The Major Commission of Inquiry and the Iacobucci Internal Inquiry /22
- Review methodology /23

In Closing /23

Annex A: Mandate of the Communications Security Establishment Commissioner /25

Annex B: Classified Reports, 1996–2007 /27

Annex C: Statement of Expenditures, 2006-2007 /31

Annex D: History of the Office of the Communications Security Establishment Commissioner /33

Annex E: Role and Mandate of the Communications Security Establishment /35

INTRODUCTION

This is my first report as Communications Security Establishment (CSE) Commissioner, since my appointment effective August 1, 2006. I have a three-year mandate that expires in August 2009.

My own background includes 30 years' experience on the bench, most recently as a Supreme Court Justice from 1989-2003. I believe there are strong parallels between the role of a judge and that of the CSE Commissioner. A judge's fundamental concern is to ensure fair trials and protect personal liberty, while maintaining peace and security. Correspondingly, the CSE Commissioner's fundamental concern is to balance the right to privacy with the need for information to protect national security. The similarity between these roles is reflected in the legislation specifying that the Commissioner be a supernumerary judge or a retired judge of a superior court.

The CSE Commissioner's fundamental concern is to balance the right to privacy with the need for information to protect national security.

There is, however, an important difference in context. While secrecy issues do arise in court proceedings in certain instances, for the most part the judicial process takes place in public. Secrecy, on the other hand, is at the very heart of foreign intelligence collection. Nevertheless, the balancing principles are the same. I see the role of my office as providing Canadians with the assurance that the CSE's critical intelligence work is being carefully examined by an impartial authority to ensure it is lawful, and that their rights are being protected, without compromising the secrecy required to protect national security.

In October 2006, I was presented with an exceptional opportunity to attend the International Intelligence Review Agencies Conference in Cape Town, South Africa. One of the conference themes was the need to balance the traditional rights and liberties of citizens with the need for increased powers to meet threats to national security. It was a remarkable experience to meet with the practitioners in security and intelligence review from 14 countries, including my own, and to hear from them first-hand about the challenges we all face. I remain grateful for this

opportunity because it provided an occasion for me, as the new CSE Commissioner, to become totally immersed in topics of mutual interest in the company of experts.

During the early days following my appointment, I met the Minister of National Defence and the Chief of CSE. I was also provided with extensive briefings and tours, many of them at CSE, and I am particularly grateful to my briefers for their comprehensive presentations. As time progressed, I had the opportunity to meet other federal government officials, including the Auditor General of Canada and the Privacy Commissioner, the Chairs of the Security Intelligence Review Committee and the Commission for Public Complaints Against the RCMP, the Deputy Minister of National Defence, and the National Defence Ombudsman.

Most important, of course, has been the time I have spent involving myself in the work of my office, and familiarizing myself with the activities and preoccupations of my predecessors, which will be discussed later in this report.

THE REVIEW ENVIRONMENT

A number of key issues helped shape the environment in which this office carried out its work over the past year. Some of these have been described and commented on by my predecessors in past Annual Reports. Below, I draw attention to some themes that have not been mentioned before, as well as some new developments in ongoing issues.

Legal interpretations

Since the omnibus *Anti-Terrorism Act* was proclaimed in December 2001, the persons who have occupied the position of CSE Commissioner have faced a persistent dilemma arising from the amendments this Act introduced to the *National Defence Act*. Particularly troublesome has been the Commissioner's duty to review the activities of CSE conducted under ministerial authorizations issued for the sole purpose of obtaining foreign intelligence, given the lack of agreement on the interpretation of key provisions of the Act.

On the one hand, my predecessors and I have recognized the importance of CSE's work, and the benefit the Government of Canada derives from the foreign intelligence CSE provides, particularly during a time when the threat of global terrorism continues unabated, and the safety of our soldiers in Afghanistan remains at risk.

On the other hand, during our respective terms as Commissioner, each of us has been unequivocal in the position that the legal interpretation and advice regarding ministerial authorizations provided to CSE by the Department of Justice is not supported by a simple reading of the appropriate provisions of Part V.1 of the *National Defence Act*, and each of us so advised the Minister of National Defence of the day. In addition, my immediate predecessor, the Right Honourable Antonio Lamer and I both made our positions known to officials at the Office of the Attorney General of Canada.

When I am asked to consider whether an activity is lawful, I must first determine what the law states in respect of that activity. The relevant Act, then, is the yardstick by which the lawfulness of the activity is measured. The difficulty arises, in instances such as this, when there is a fundamental difference of opinion about what the Act states.

I do not question the role of the Department of Justice in the drafting of legislation, nor do I view my role as Commissioner as arbiter of statutory interpretation. However, as I have informed the Minister of National Defence and the Attorney General of Canada, the legislation lacks clarity and it ought to be amended, a view I share with both my predecessors.

The legislation lacks clarity and it ought to be amended.

This matter has been under deliberation for some time, and I hope the government will make the required amendments at the earliest opportunity. I am confident that this will not be too onerous a task because other countries have successfully adopted and are applying legislation to meet similar requirements.

Legislation lagging behind technological advances

As time goes on, there is an ever-widening knowledge gap between the general public and evolving technologies. In a number of respects, Canada's laws have also not kept pace with technological advances. We need a more imaginative approach. Today, criminal and terrorist elements are masters of these complex technologies and, unlike democratic institutions, are unimpeded by legal constraints. Those involved in the legislative process need to avoid laws that are driven by the technology of the day, which will in short order be superseded by new developments. Instead, we must ensure our laws have a broad enough scope, and are so structured — be it by providing for regulations or otherwise — that they can accommodate new technologies, and continue to protect both our privacy and security.

Three-year review of the *Anti-Terrorism Act*

The *Anti-Terrorism Act* amended the *Official Secrets Act* and the *National Defence Act*, among other legislation. The amendments to the *National Defence Act* included a legislative basis for CSE and the CSE Commissioner.

The *Anti-Terrorism Act* required a review of its provisions and operation within three years of receiving royal assent, to be carried out by a designated or specially established committee of the Senate or the House of Commons, or of both chambers. A Subcommittee of the House of Commons Standing Committee on Public Safety and National Security was established for this purpose in autumn 2004. At the same time, the Senate established a Special Committee to carry out a comprehensive review of the Act. As described in the 2005-2006 Annual Report, my predecessor appeared before the Senate Special Committee on June 13, 2005, and two days later before the House of Commons Subcommittee. The Senate Special Committee reported on February 22, 2007, and the House Subcommittee reported on March 27, 2007.

Senate Special Committee recommendations

The Senate Special Committee made several recommendations concerning CSE as well as this office. As regards CSE, the Committee focussed primarily on ministerial authorizations, stating that it accepted the explanations as to why CSE needs to intercept private communications when undertaking its foreign intelligence and information technology security activities. It also accepted Commissioner Lamer's explanation that ministerial authorizations were the proper instrument to use for intercepting private communications, rather than prior judicial authorization, because warrants from Canadian courts have no jurisdiction outside Canada.[1] The Committee drew comfort from the fact that this office is required to review the lawfulness of CSE's activities, including the interception of private communications under ministerial authorizations. However, it remained concerned, as was Commissioner Lamer, that the standard required to satisfy the Minister that all necessary preconditions to intercepting private communications have been met is unclear. Accordingly, the Committee recommended that subsections 273.65(2) and (4) of the *National Defence Act* be amended to clarify whether these preconditions should be based on reasonable belief or reasonable suspicion.[2] This has been an issue of interest to my office, and a clarification would be welcome.

The Committee drew comfort from the fact that this office is required to review the lawfulness of CSE's activities.

Because the Committee wished to ensure that intercepted information is disposed of if it has been determined to be non-essential or when it is no longer essential, it recommended that CSE develop information retention and disposal policies, containing specific timeframes for the disposal of intercepted information, and that it make these policies publicly available.[3]

---

[1] Special Senate Committee on the *Anti-Terrorism Act*, *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the* Anti-Terrorism Act, February 2007, p. 77.
[2] *Ibid.*, Recommendation 18, p. 78.
[3] *Ibid.*, Recommendation 19, p. 79.

In the interests of accountability and transparency, the Committee also recommended that the Minister of National Defence or the CSE be required to report annually to Parliament on the number of ministerial authorizations issued during the year, the number still in force by the end of the year, and the general purpose for which each authorization was issued (i.e., to obtain foreign intelligence or to protect computer systems or networks).[4]

The *Anti-Terrorism Act* also amended the *Official Secrets Act*, and renamed it the *Security of Information Act*, known as SOIA. SOIA establishes a process that persons permanently bound to secrecy must follow if they wish to claim a public interest defence for divulging classified information. The Commissioner may receive classified information as part of the process (see Annex A). However, the *Security of Information Act* does not describe what should be done once the Commissioner receives that information.[5] The Committee recommended that the Government specify the procedure to be followed in such cases.[6] I should point out that my office does have internal policies and procedures in place to fill the gap that the Committee identified.

Lastly, the Committee discussed the oversight and review of Canada's national security and anti-terrorism framework. The Committee mentioned that this office is "generally perceived to be an effective oversight mechanism."[7] The Committee recommended that a standing Senate committee be established to monitor and periodically report on Canada's anti-terrorism legislation and national security framework on an ongoing basis. In addition, the Committee called for a comprehensive parliamentary review of the provisions and operation of the *Anti-Terrorism Act* every five years.

---

[4] *Ibid.*, Recommendation 20, p. 79.
[5] To date, I have not received any information under the *Security of Information Act*.
[6] *Supra*, footnote 1, Recommendation 26, p. 94.
[7] *Supra*, footnote 1, p.116.

House of Commons Subcommittee recommendations

The House Subcommittee's Final Report on its review of the *Anti-Terrorism Act* also addressed the issue of ministerial authorizations. In particular, I was pleased to note that the Subcommittee drew attention to the remarks of my predecessor in his 2005-2006 Annual Report about the legal ambiguities and uncertainties in the provisions allowing for ministerial authorizations, and the disagreement regarding interpretation of these provisions between this office and the Department of Justice. Without making a specific recommendation in this regard, the Subcommittee urged government counsel and me to resolve these issues as expeditiously as possible. As well, the Subcommittee requested that the Government's response to the Final Report indicate what the issues of disagreement are and how they have been resolved, to the extent possible. Failing this, the Subcommittee believes I should provide these details in my 2007-2008 Annual Report.[8] I intend to revisit this recommendation as the time for that report approaches.

My office's review methodology always includes an examination of compliance with the Charter and the Privacy Act.

The Subcommittee also supported a recommendation by the Privacy Commissioner that subsection 273.65(8) of the *National Defence Act* be amended to require the CSE Commissioner to review the private communication interception activities carried out under ministerial authorization to ensure they comply with the requirements of the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*, as well as with the authorization itself. This position was reinforced with an additional recommendation that section 273.66 of the *National Defence Act* be amended to require the CSE only to undertake activities consistent with the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*, in addition to the restraints on the exercise of its mandate already set out in that section.[9] I should point out that my office's review methodology always includes an examination of compliance with the *Charter* and the *Privacy Act*.

---

[8] Subcommittee on the Review of the *Anti-Terrorism Act*, *Rights, Limits, Security: A Comprehensive Review of the* Anti-terrorism Act *and Related Issues. Final Report of the Standing Committee on Public Safety and National Security*, March 2007, p. 56.

[9] *Ibid.*, Recommendations 44 and 45, pp. 55-56.

With respect to the issue of review and oversight, the Subcommittee recommended that Bill C-81 from the 38th Parliament, the proposed *National Security Committee of Parliamentarians Act*, or a variation of it, be introduced in Parliament at the earliest opportunity. The Subcommittee further recommended that the mandate of the proposed committee include undertaking compliance audits of departments and agencies, such as CSIS, CSE, and national security elements of the RCMP, in relation to the provisions of the *Anti-Terrorism Act*.[10] In last year's Annual Report, my predecessor welcomed the prospect of more active parliamentary review of national security activities, but also noted challenges such as the composition of the committee and its access to classified information and documents. I concur with that position in general, and intend to offer specific comments once a bill is introduced.

Finally, the Subcommittee recommended that there be another comprehensive review of the provisions and operation of the *Anti-Terrorism Act*, to begin no later than December 31, 2010, and to be completed no later than December 31, 2011. It noted that the proposed committee of parliamentarians would be well-equipped to carry out this review.[11]

The O'Connor Commission of Inquiry

The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar was established February 5, 2004. It was mandated to investigate and report on the actions of Canadian officials in relation to Maher Arar (Factual Inquiry) as well as to recommend an arm's-length review mechanism for the activities of the RCMP with respect to national security (Policy Review). The Honourable Dennis O'Connor was appointed Commissioner of the Inquiry. He released his Policy Review report on December 12, 2006.

[10] *Ibid.*, Recommendations 58 and 59, pp. 84-86.
[11] *Ibid.*, pp. 83-85.

In order to provide integrated review of integrated national security activities, Commissioner O'Connor recommended that statutory gateways be enacted linking the proposed Independent Complaints and National Security Review Agency for the RCMP, the Security Intelligence Review Committee and the Office of the CSE Commissioner to provide for exchange of information, referral of investigations, conduct of joint investigations, and coordination and preparation of reports.[12] I welcome this proposal, although to date the absence of gateways has never been an operational impediment.

I was pleased to note the following observation from Justice O'Connor's report: "I am not recommending that SIRC's mandate be expanded to include the CSE, as I understand that the Office of the CSE Commissioner functions very well and I see no reason to interfere with that operation."[13] I was also pleased to see that my office was recognized for the creation of the Review Agencies Forum in 2005-2006.[14] The Forum is described further on in this report.

I do have reservations, however, regarding Justice O'Connor's recommendation to establish an Integrated National Security Review Coordinating Committee.[15] I am concerned that introducing such a coordinating committee by way of statute, and amendments to related legislation, may create an unnecessary and counter-productive level of bureaucracy between independent review agencies and Parliament.

[12] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006), p. 578.
[13] *Ibid.*, Recommendation 11, p. 580.
[14] *Ibid.*, p. 282.
[15] *Ibid.*, Recommendation 12, p. 591.

THE YEAR IN REVIEW

Independent Reviews of OCSEC

In spring 2006, two independent management reviews of my office were commissioned. One focussed on administration, including the management and control of financial, human and information resources. The other dealt with operations, by assessing whether the office carries out the Commissioner's mandated responsibilities efficiently and effectively.

I was pleased to note that the findings of the administrative review were all positive.

The reports of these management reviews were available to me at the time of my appointment, thus providing me with an independent assessment of my new area of responsibility. I was pleased to note that the findings of the administrative review were all positive. The recommendations of the operational review were discussed in detail at a review workshop held on August 21, 2006, with the review consultants as moderators. The operational review also raised methodology issues, which will be briefly referred to later in this report.

Workplan

My office's activities are guided by a regularly updated three-year workplan. To facilitate scheduling, my staff consult with CSE about the review components of this plan. Criteria that determine their selection of topics for review include: CSE activities or programs that have not previously or recently been reviewed; areas identified from briefings requested of CSE; the status of recommendations from previous reviews; and activities where privacy is most likely to be at risk. My staff, who have extensive knowledge of CSE, ask themselves fundamental questions such as: what can go wrong; what is the probability of something going wrong; and what are the consequences if they do go wrong.

Also during the year, considerable staff time and resources were devoted to work on legal interpretation issues, which I have already described in detail above in my discussion of the review environment.

Reviews undertaken of CSE

My general review mandate is set out in paragraph 273.63(2)(a) of the *National Defence Act*.[16] Under subsection 273.65(8) of the Act, I also have an obligation to review and report to the Minister as to whether the activities carried out under a ministerial authorization are authorized.

Ministerial authorizations for foreign intelligence collection are issued under the authority of subsection 273.65(1) of the *National Defence Act*, whereas ministerial authorizations for information technology security activities are issued under subsection 273.65(3) of the Act. Reviews of CSE's activities conducted under ministerial authorizations are undertaken only after the ministerial authorization has expired.

During 2006-2007, my office submitted classified reports of four reviews to the Minister. Two of the reviews dealt with CSE's activities conducted under ministerial authorization; one pertained to foreign intelligence collection, while the other concerned information technology security. The other two reviews were conducted under my general mandate, to ensure the activities were in compliance with the law.

[16] Please see Annex A for the text of the relevant sections of the *National Defence Act*.

2006-2007 REVIEW HIGHLIGHTS

Review of CSE's foreign intelligence collection in support of the RCMP

Background

In January 2005, my office submitted a report to the Minister of National Defence examining the technical and operational assistance CSE provided to the RCMP under paragraph 273.64(1)(c) of the *National Defence Act*, also known as mandate (c).[17] The second and final phase of the review was completed and in June 2006, my predecessor submitted a follow-up report reviewing CSE's foreign signals intelligence collection activities in support of the RCMP under pararagraph 273.64(1)(a) of the *National Defence Act*, also known as mandate (a). Further details on the first phase of the review may be obtained in the 2004-2005 Annual Report of this office.

Under mandate (a), CSE provides two kinds of foreign intelligence information to its government clients, including the RCMP. Most of its reports address general areas of interest that complement and support the client's own mandated responsibilities. In addition to this proactive support, CSE provides reactive support by responding to specific requests by the client for intelligence-related information.

Methodology

OCSEC staff examined CSE's mandate (a) activities in support of the RCMP for the period January 1 to December 31, 2003. They received briefings and answers to both verbal and written questions that were posed to CSE officials. They also obtained a listing of the agency's requests for intelligence-related information and chose several to examine in detail. As part of this in-depth examination, two separate demonstrations illustrating the activities under review were provided to OCSEC staff by those CSE officials who had been directly involved in responding to the requests.

[17] CSE's mandate is described in Annex E of this report.

Findings

Many of the findings and recommendations made in my office's first report also applied to this second-phase review of assistance provided under mandate (a). For example, it was recommended CSE amend and/or update the instruments that guide its support activities to the RCMP. My predecessor was pleased to report that, for the most part, CSE had accepted these recommendations and is working to implement them.

CSE has advised that high priority has been given to the development and implementation of a corporate records management system.

CSE also acknowledged the need to implement a formal system of record keeping. This is a continuing concern, as was noted in my office's 2005-2006 Annual Report. CSE has advised that high priority has been given to the development and implementation of a corporate records management system that will deal with their hard-copy and electronic records requirements.

During the second phase of the review, a detailed examination of CSE's response to RCMP requests for intelligence-related information identified two issues of concern that required further legal study by CSE. The first was whether mandate (a) was the appropriate authority in all instances for CSE to provide intelligence support to the RCMP in the pursuit of its domestic criminal investigations. Pending a re-examination of this issue by CSE, no assessment was made of the lawfulness of CSE's activities in support of this agency under mandate (a) as currently interpreted and applied by CSE. My staff is monitoring the issue.

The second issue related to CSE's policies and practices as they relate to the disclosure of Canadian personal information to its clients. When collecting foreign intelligence, CSE may incidentally acquire personal information about Canadians. This information may be retained if assessed as essential to the understanding of the foreign intelligence, and it may be included in foreign intelligence reporting if it is suppressed (i.e. replaced by a generic reference such as "a Canadian person"). When receiving a subsequent request for disclosure of the full details of Canadian personal information, CSE requires its clients, including the

RCMP, to justify their authority to collect this information under their own respective mandates and provide an operational justification of their need to know this information. If these conditions are met, CSE releases the information.

An in-depth examination of relevant sections of the *National Defence Act* and the *Privacy Act* raised questions as to CSE's conformance with the various authorities that govern disclosure. Thus, my office recommended that CSE also re-examine its authority to collect, use and disclose personal information to certain federal government departments and agencies. In addition, my office has recommended that CSE establish agreements with client agencies to formalize the circumstances when such information may be disclosed while providing assistance under its (c) mandate.

CSE acknowledged that the report "raises a number of issues that, from a policy/legal perspective, will generate further in-depth analysis by CSE and Department of Justice legal counsel." I anticipate that this analysis will include a discussion and perhaps even a formal articulation by CSE of its position regarding the application of the *National Defence Act* as it relates to the provision of foreign intelligence in accordance with the Government of Canada intelligence priorities.

Review of information technology security activities at a government department

Background

This review examined information technology security activities conducted by CSE under ministerial authorization in 2004-2005 at a government department. The objective was to assess and verify compliance with the law and with the provisions of the ministerial authorization for these activities.

Individuals conducting personal and business affairs with the Government of Canada have a reasonable expectation of privacy. However, when the security of government computer systems and networks is being tested, personal information or private communications can be inadvertently intercepted with certain types of necessary testing. Subsection 273.65(3) of the *National Defence Act* provides that:

Individuals conducting personal and business affairs with the Government of Canada have a reasonable expectation of privacy.

> The Minister may, for the sole purpose of protecting the computer systems or networks of the Government of Canada from mischief, unauthorized use or interference, in the circumstances specified in paragraph 184(2)(c) of the *Criminal Code*, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization.

In such cases, CSE is responsible for seeking authorization on behalf of the department or agency requesting the activity to be covered. This ministerial authorization enables CSE to undertake a complete assessment of a department's computer systems and networks.

Methodology

The review was conducted initially through examination of documents and files related to the ministerial authorization and the conditions imposed by it. Fact-finding and verification interviews were then held with CSE and selected client representatives who were identified as having direct involvement in the authorization process or ensuing activities.

Findings

With the qualification set out below regarding one of the conditions of the ministerial authorization, this review found that CSE's work at the department was in compliance with the law and with the ministerial authorization.

The review found that the process by which CSE acquired the information technology security ministerial authorization for its activities at the department was found to be in accordance with the requirements of the *National Defence Act*. It was also determined that four of the five conditions set out in subsection 273.65(4) of the Act were complied with satisfactorily. However, with respect to one of the conditions, the review found that certain information was retained even though its retention was not essential. While CSE personnel acted in a manner that was consistent with the direction they were given, there were aspects that could be improved upon, and CSE has undertaken to do so. CSE has also indicated that future Memoranda of Understanding with client departments where information technology security activities under ministerial authorizations are to be conducted will reflect these improvements.

Other recommendations from the review included ensuring that future policy and practice promote conformance with CSE's legislated authorities as they relate to staff activities during information technology security exercises.

Review of the roles of CSE's client relations officers and the Operational Policy Section in the release of personal information

Background

The objective of this review was to assess the lawfulness of the activities of both the CSE client relations officers and the Operational Policy Section, as they relate to the request for and release of personal information about Canadians that has been suppressed in CSE foreign intelligence reports, as referred to previously. This information is made available to authorized Government of Canada clients, only under certain conditions.

CSE has provided foreign intelligence reports based on signals intelligence to officials in government departments since its formal establishment in 1946. Reports were delivered by hand until the creation of the on-site client relations officer programme in 1985. Client relations officers provide intelligence reports, explain to individual clients and potential

clients the role of CSE and signals intelligence, and assist in determining client needs based on Government of Canada intelligence priorities.

To protect privacy, CSE suppresses personal information about Canadians in foreign intelligence reports. If a client has both the authority and the need to know the information, it must make a formal request and provide justification. Requests for release of this information are centralized in CSE's Operational Policy Section.

To protect privacy, CSE suppresses personal information about Canadians in foreign intelligence reports.

The majority of requests are now made via a secure communication network directly to CSE. Client relations officers play a role in the release of Canadian identities in CSE foreign intelligence reports because they continue to deal with requests from clients who do not have access to this secure network.

Methodology

This review examined relevant documentation, including the authorities that govern the activities of client relations officers and the CSE unit authorized to release this information. All requests for and releases of suppressed information during a six-month period were reviewed in detail to ensure compliance with law and policy. Interviews were conducted with client relations officers, their managers, and the manager of the Operational Policy Section.

Findings

The review concluded that the activities of the CSE client relations officers and the Operational Policy Section were in compliance with the *National Defence Act* and with CSE's related policies. There were some inconsistencies in requests and releases, as well as areas where both policy and practice could be improved to enhance the protection of privacy, as required by the *Privacy Act*. Recommendations included more comprehensive training for clients who make requests, and providing more clients with secure, electronic access to CSE as a means of reducing errors and enhancing control over the process. I was pleased to note that

since the period of review there has also been increased training for and supervision of personnel in the Operational Policy Section at CSE as regards the release of suppressed information.

Review of CSE signals intelligence collection activities conducted under ministerial authorizations

Background

Certain foreign intelligence collection activities were conducted under three ministerial authorizations that were in effect from March 2004 to December 2006. These ministerial authorizations focused on acquiring communications of foreign intelligence value from the global information infrastructure.[18]

The characteristics of contemporary communications technology mean that the interception of communications by CSE, directed at foreign entities outside Canada, runs the inherent risk of acquiring the private communications of Canadians. It is for this reason that a ministerial authorization is sought for this collection. In addition to the conditions set out in subsection 273.65(2) of the *National Defence Act*, a ministerial directive established other conditions for managing the collection.

My office is undertaking a two-part review of the activities under these ministerial authorizations, as the law is interpreted by the Department of Justice, a point which is discussed below. The objective of this first phase was to provide background to, and criteria for, the detailed review of these complex activities. I provided the Minister of National Defence with a brief report on this study phase in February 2007.

[18] "Global information infrastructure" includes electromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in, or relating to those emissions, systems or networks. (*National Defence Act*, section 273.61)

Methodology

In order to establish an understanding of this foreign intelligence collection and the unique challenges it presents, this first phase of the review: studied the authorities given to and the conditions imposed upon CSE by the ministerial authorizations, ministerial directive and related articles; and examined how CSE has responded in terms of the policies and procedures that it has developed, and the management framework that has been put in place to oversee these activities.

Findings

This study phase developed an historical perspective and appreciation of the rationale for this collection activity. It also provided an appreciation of the organizational complexities, the authorities under which it operates, the conditions imposed and the programs in place to implement the authorities while respecting the conditions. Finally, it established the review criteria for the second and final phase, which is now underway.

Overview of 2006-2007 findings

I am able to report that, overall, the activities of CSE examined during this reporting period complied with the law, with one qualification. It concerned a condition of an information technology security ministerial authorization, which CSE has already undertaken to rectify. A report of CSE's assistance to the RCMP did not provide an assessment of the lawfulness of the activities reviewed, pending a re-examination by CSE of the legal issues raised.

With respect to the review of CSE's signals intelligence collection activities conducted under ministerial authorization, I would highlight once again my disagreement with the Department of Justice's interpretation of the ministerial authorization provisions of the *National Defence Act*. When assessing the lawfulness of activities conducted under ministerial authorizations, I have agreed to use the Department of Justice's interpretation for the present pending amendments to the legislation, which I have already urged be made at the earliest opportunity. I commend the Chief of CSE for supporting this initiative.

Reviews underway / future reporting

Reviews currently underway that I will be reporting on in the next fiscal year include examinations of CSE's activities related to counter-terrorism, its use of metadata, its support to CSIS, its use of technology to protect the privacy of Canadians, and its activities under a number of foreign intelligence collection and information technology security ministerial authorizations. In addition, my office will begin a number of other reviews, under both my general mandate and my duties under the ministerial authorization provisions.

Complaints about CSE activities

My mandate includes undertaking any investigation I deem necessary in response to a complaint, to determine whether CSE engaged, or is engaging in unlawful activity.

During the 2006-2007 reporting year my office received no complaints that warranted formal investigation. However, OCSEC did complete one investigation in spring 2006 in response to a complaint that was received in the previous reporting year. A full report was delivered to the Minister of National Defence outlining the facts of the complaint and the findings resulting from the investigation.

I am able to report that the investigation found no unlawful activity on the part of CSE.

While the substance of the complaint is classified, I am able to report that the investigation found no unlawful activity on the part of CSE. My office made recommendations that were accepted by CSE, and would strengthen compliance.

Duties under the *Security of Information Act*

I have a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy if they wish to claim a "public interest" defence for divulging classified information. No such matters were referred to my office in 2006-2007.

THE COMMISSIONER'S OFFICE

I am supported in my work by a full-time staff of eight. Their extensive experience in the security and intelligence community is supplemented by subject matter experts in areas such as informatics, technology, research, policy development and communications, with whom my office contracts as required.

Many of my office's interests and concerns are shared by other Canadian security and intelligence review agencies. As Justice O'Connor noted, in 2005-2006 my staff initiated the Review Agencies Forum, which brings them together at regular intervals with the staffs of the Security Intelligence Review Committee, the Office of the Inspector General of the Canadian Security Intelligence Service and the Commission for Public Complaints Against the RCMP. In 2006-2007, the Forum met twice to discuss issues such as the recommendations of Justice O'Connor's Policy Review report, and amendments to the *Public Servants Disclosure Act* resulting from the new *Federal Accountability Act* (Bill C-2). In addition, Forum participants discussed how to provide their respective agencies with reasonable turnaround times in responding to reviews, and the different approaches that have been used when delays are encountered.

My staff also participated in other conferences and symposia that provided them with new perspectives on their work, including the International Intelligence Review Agencies Conference in Cape Town, which I described above, and the conferences of the Canadian Association for Security and Intelligence Studies (CASIS) and the Ontario Bar Association. In addition, as a developmental opportunity, my office hosted two promising students at the CASIS conference.

In 2006-2007, there were some 96,000 visits to my website.

While my office does not have a formal educational mandate, I do believe it is important that Canadians know about OCSEC's work. To this end, my office hosts a website (www.csec-ccst.gc.ca) that describes OCSEC's mandate and activities. Visits to the site originating from outside North America span a global audience ranging from Europe to Asia and the Middle East. In 2006-2007, there were some 96,000 visits to my website.

In 2006-2007, my office's expenditures were $ 1,267,612, which was well within budget for the period. Annex C to this report provides a summary of 2006-2007 expenditures.

LOOKING TO THE FUTURE

The Major Commission of Inquiry and the Iacobucci Internal Inquiry

Two new inquiries that may have an impact on the future review environment are the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, led by the Honourable John Major, and the Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, led by the Honourable Frank Iacobucci.

The Air India Commission's mandate is to make findings and recommendations regarding the assessments and actions of Canadian government officials before and after the 1985 bombing, and ways that any past mistakes can be avoided in the future. The Internal Inquiry is mandated to examine all aspects of the involvement of Canadian officials in relation to the detention of the three individuals in Syria or Egypt.

Review methodology

One of the recommendations of the independent operational review of my office conducted in spring 2006 was to document formally the methodology employed by the office to examine CSE's activities. I support this initiative entirely and I am confident that the office will derive benefit from it now and in the longer term. This will be an important preoccupation over the summer months.

IN CLOSING

Looking back over the last eight months, I would like to express appreciation to my predecessor, the Right Honourable Antonio Lamer, from whom I inherited a fine staff and an organization well positioned to meet the challenges ahead. Thanks to this legacy, I was able to assume my responsibilities immediately upon my appointment, and the transition between our tenures was seamless.

I anticipate continuing the productive relationships that have been established.

I anticipate continuing the productive relationships that have been established with the Minister of National Defence, with CSE and with officials at other government departments and agencies involved in Canada's security and intelligence community. In particular, I look forward to discussions that I trust will lead to a resolution of the legal interpretation issues that have beset this office since the passage of Part V.1 of the *National Defence Act*.

ANNEX A: MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

***National Defence Act* – Part V.1**

273.63 (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

(2) The duties of the Commissioner are

(a) to review the activities of the Establishment to ensure that they are in compliance with the law;

(b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

[...]

273.65 (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

Security of Information Act

15. (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest. [...]

(5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following: [...]

(b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, [...]

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.

ANNEX B: CLASSIFIED REPORTS, 1996–2007

1. Classified Report to the Minister
   – March 3, 1997 (TOP SECRET)

2. Classified Report to the Minister
   – Operational policies with lawfulness implications – February 6, 1998 (SECRET)

3. Classified Report to the Minister
   – CSE's activities under *** – March 5, 1998 (TOP SECRET Codeword/CEO)

4. Classified Report to the Minister
   – Internal investigations and complaints – March 10, 1998 (SECRET)

5. Classified Report to the Minister
   – CSE's activities under *** – December 10, 1998 (TOP SECRET/CEO)

6. Classified Report to the Minister
   – On controlling communications security (COMSEC) material – May 6, 1999 (TOP SECRET)

7. Classified Report to the Minister
   – How we test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) – June 14, 1999 (TOP SECRET Codeword/CEO)

8. Classified Report to the Minister
   – A study of the *** collection program – November 19, 1999 (TOP SECRET Codeword/CEO)

9. Classified Report to the Minister
   – On *** – December 8, 1999 (TOP SECRET/COMINT)

10. Classified Report to the Minister
    – A study of CSE's *** reporting process — an overview (Phase I)
    – December 8, 1999 (SECRET/CEO)

11. Classified Report to the Minister
    – A study of selection and *** — an overview – May 10, 2000 (TOP SECRET/CEO)

12. Classified Report to the Minister
    – CSE's operational support activities under *** — follow-up – May 10, 2000 (TOP SECRET/CEO)

13. Classified Report to the Minister
    – Internal investigations and complaints — follow-up – May 10, 2000 (SECRET)

14. Classified Report to the Minister
    – On findings of an external review of CSE's ITS program – June 15, 2000 (SECRET)

15. Classified Report to the Minister
    – CSE's policy system review – September 13, 2000 (TOP SECRET/CEO)

16. Classified Report to the Minister
    – A study of the *** reporting process — *** (Phase II) – April 6, 2001 (SECRET/CEO)

17. Classified Report to the Minister
    – A study of the *** reporting process — *** (Phase III) – April 6, 2001 (SECRET/CEO)

18. Classified Report to the Minister
    – CSE's participation *** – August 20, 2001 (TOP SECRET/CEO)

19. Classified Report to the Minister
    – CSE's support to ***, as authorized by *** and code-named ***
    – August 20, 2001 (TOP SECRET/CEO)

20. Classified Report to the Minister
    – A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS)
    – August 21, 2002 (SECRET)

21. Classified Report to the Minister
    – CSE's support to ***, as authorized by *** and code-named ***
    – November 13, 2002 (TOP SECRET/CEO)

22. Classified Report to the Minister
    – CSE's *** activities carried out under the *** 2002 *** Ministerial authorization – November 27, 2002 (TOP SECRET/CEO)

23. Classified Report to the Minister
    – Lexicon of CSE definitions – March 26, 2003 (TOP SECRET)

24. Classified Report to the Minister
    – CSE's activities pursuant to *** Ministerial authorizations including *** – May 20, 2003 (SECRET)

25. Classified Report to the Minister
    – CSE's support to ***, as authorized by *** and code-named *** — Part I – November 6, 2003 (TOP SECRET/COMINT/CEO)

26. Classified Report to the Minister
    – CSE's support to ***, as authorized by *** and code-named *** — Part II – March 15, 2004 (TOP SECRET/COMINT/CEO)

27. Classified Report to the Minister
    – A review of CSE's activities conducted under *** Ministerial authorization – March 19, 2004 (SECRET/CEO)

28. Classified Report to the Minister
    – Internal investigations and complaints — follow-up – March 25, 2004 (TOP SECRET/CEO)

29. Classified Report to the Minister
    – A review of CSE's activities conducted under 2002 *** Ministerial authorization – April 19, 2004 (SECRET/CEO)

30. Classified Report to the Minister
    – Review of CSE *** operations under Ministerial authorization – June 1, 2004 (TOP SECRET/COMINT)

31. Classified Report to the Minister
    – CSE's support to *** – January 7, 2005 (TOP SECRET/COMINT/CEO)

32. Classified Report to the Minister
    – External review of CSE's *** activities conducted under Ministerial authorization – February 28, 2005 (TOP SECRET/COMINT/CEO)

33. Classified Report to the Minister
    – A study of the *** collection program – March 15, 2005 (TOP SECRET/COMINT/CEO)

34. Classified Report to the Minister
    – Report on the activities of CSE's *** – June 22, 2005 (TOP SECRET)

35. Classified Report to the Minister
    – Interim report on CSE's *** operations conducted under Ministerial authorization – March 2, 2006 (TOP SECRET/COMINT)

36. Classified Report to the Minister
    – External review of CSE *** activities conducted under Ministerial authorization – March 29, 2006 (TOP SECRET/CEO)

37. Classified Report to the Minister
    – Review of CSE's foreign intelligence collection in support of the RCMP (Phase II) – June 16, 2006 (TOP SECRET/COMINT/CEO)

38. Classified Report to the Minister
    – Review of information technology security activities at a government department under ministerial authorization – December 18, 2006 (TOP SECRET)

39. Classified Report to the Minister
    – Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – February 20, 2007 (TOP SECRET/COMINT/CEO)

40. Classified Report to the Minister
    – Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – March 31, 2007 (TOP SECRET/COMINT/CEO)

ANNEX C: STATEMENT OF EXPENDITURES 2006–2007

Standard Object Summary

Salaries and Wages	$594,551
Transportation and Telecommunications	72,839
Information	14,071
Professional and Special Services	402,620
Rentals	140,315
Purchased Repair and Maintenance	4,649
Materials and Supplies	6,404
Acquisition of Machinery and Equipment	29,977
Other Expenditures	2,186
Total	**$1,267,612**

ANNEX D: HISTORY OF THE OFFICE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

The Office of the Communications Security Establishment Commissioner (OCSEC) was created on June 19, 1996, with the appointment of the inaugural Commissioner, the Honourable Claude Bisson, O.C., a former Chief Justice of Quebec, who held the position until June 2003. He was succeeded by the Right Honourable Antonio Lamer, P.C., C.C., C.D., LL.D., D.U., Chief Justice of Canada (retired) for a term of three years. The Honourable Charles D. Gonthier, Q.C., who retired as Justice of the Supreme Court of Canada in 2003, was appointed as Commissioner in August 2006.

For the first six years (from June 1996 to December 2001), the Commissioner carried out his duties under the authority of Orders in Council issued pursuant to Part II of the *Inquiries Act*. During this period, the Commissioner's responsibilities were twofold: to review the activities of the Communications Security Establishment (CSE) to determine whether they conformed with the laws of Canada; and to receive complaints about CSE's activities.

Following the terrorist attacks in the United States on September 11, 2001, Parliament adopted the omnibus *Anti-Terrorism Act* which came into force on December 24, 2001. The omnibus *Act* introduced amendments to the *National Defence Act*, by adding Part V.1 and creating legislative frameworks for both OCSEC and CSE. It also gave the Commissioner new responsibilities to review activities carried out by CSE under a ministerial authorization.

The omnibus legislation also introduced the *Security of Information Act*, which replaced the *Official Secrets Act*. This legislation gives the Commissioner specific duties in the event that a person, who would otherwise be permanently bound to secrecy, seeks to defend the release of classified information about CSE on the grounds that it is in the public interest.

Under the Commissioner's current mandate, which entrenched in law the original mandate established in 1996 as well as the additional responsibilities described above, the Commissioner has retained the powers of a commissioner under Part II of the *Inquiries Act*.

ANNEX E: ROLE AND MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT

The Communications Security Establishment (CSE) is Canada's national cryptologic agency. Unique within Canada's security and intelligence community, CSE employs code-makers and code-breakers to provide the Government of Canada with information technology security and foreign signals intelligence services. CSE also provides technical and operational assistance to federal law enforcement and security agencies.

CSE's foreign signals intelligence products and services support government decision-making in the fields of national security, national intelligence and foreign policy. CSE's signals intelligence activities relate exclusively to foreign intelligence and are directed by the Government of Canada's intelligence priorities.

CSE's information technology security products and services enable its clients (other government departments and agencies) to effectively secure their electronic information systems and networks. CSE also conducts research and development on behalf of the Government of Canada in fields related to communications security.

CSE has a three-part mandate under Part V.1, subsection 273.64(1) of the *National Defence Act*. These are known as the (a) (b) and (c) mandates:

(a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
(b) to provide advice, guidance and services to help ensure the protection of electronic information and information infrastructures of importance to the Government of Canada; and
(c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

Commissaire
du Centre
de la sécurité
des télécommunications

Rapport annuel

2006-2007

Canada

Bureau du commissaire du Centre
de la sécurité des télécommunications
C.P. 1984,
Succursale « B »
Ottawa (Ontario)
K1P 5R5

Tél. : (613) 992-3044
Téléc. : (613) 992-4096
Site Web : http://csec-ccst.gc.ca

© Ministre des Travaux publics et des
Services gouvernementaux Canada 2007
ISBN 978-0-662-69804-3
N° de cat. D95-2007

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Charles D. Gonthier, c.r.

CANADA

Communications Security
Establishment Commissioner

The Honourable Charles D. Gonthier, Q.C.

Mai 2007

Ministre de la Défense nationale
Édifice MGen G.R. Pearkes, 13e étage
101, promenade Colonel-By, tour nord
Ottawa (Ontario)
K1A 0K2

Monsieur le Ministre,

Conformément au paragraphe 273.63(3) de la *Loi sur la défense nationale*, j'ai le plaisir de vous communiquer mon rapport annuel de 2006-2007 sur mes activités et constatations, aux fins de présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

Charles D. Gonthier

P.O. Box/C.P. 1984, Station "B"/Succursale « B »
Ottawa, Canada
K1P 5R5
(613) 992-3044 Téléc. : (613) 992-4096

TABLE DES MATIÈRES

Introduction /1

Contexte de l'examen /2
- Interprétation juridique /2
- Retard des lois sur les progrès technologiques /4
- Examen triennal de la *Loi antiterroriste* /4
- Recommandations du Comité sénatorial spécial /5
- Recommandations du Sous-comité de la Chambre des communes /7
- Commission d'enquête O'Connor /8

Rétrospective de l'année /10
- Examens indépendants du BCCST /10
- Plan de travail /10
- Examens effectués /11

Points saillants en 2006-2007 /12
- Examen des activités de collecte de renseignements étrangers effectuées par le CST à l'appui des activités de la GRC /12
  - Contexte /12
  - Méthodologie /12
  - Conclusions /13
- Examen des activités liées à la protection de la sécurité des technologies de l'information au sein d'un ministère /14
  - Contexte /14
  - Méthodologie /15
  - Conclusions /15
- Examen des rôles des agents des relations avec la clientèle et de la Section des politiques opérationnelles du CST dans la divulgation de renseignements personnels /16
  - Contexte /16
  - Méthodologie /17
  - Conclusions /17

Points saillants en 2006-2007 *(suite)*

- Examen des activités de collecte de renseignements électromagnétiques menées par le CST sous le régime d'une autorisation ministérielle /18
  - Contexte /18
  - Méthodologie /19
  - Conclusions /19
- Aperçu des conclusions pour 2006-2007 /19
- Examens en cours / rapports à venir /20
- Plaintes relatives aux activités du CST /20
- Fonctions exercées en vertu de la *Loi sur la protection de l'information* /20

Bureau du commissaire /21

Regard sur l'avenir /22

- Commission d'enquête Major et Enquête interne Iacobucci /22
- Méthodologie de l'examen /23

Conclusion /23

Annexe A : Mandat du commissaire du Centre de la sécurité des télécommunications /25

Annexe B : Rapports classifiés, 1996-2007 /27

Annexe C : État des dépenses, 2006-2007 /31

Annexe D : Historique du Bureau du commissaire du Centre de la sécurité des télécommunications /33

Annexe E : Rôle et mandat du Centre de la sécurité des télécommunications /35

INTRODUCTION

Ce rapport est le premier que je présente à titre de commissaire du Centre de la sécurité des télécommunications (CST) depuis ma nomination à ce poste le 1er août 2006. Mon mandat est d'une durée de trois ans et se termine donc au mois d'août 2009.

Mon expérience professionnelle comprend 30 ans au sein de la magistrature. J'ai notamment été juge à la Cour suprême de 1989 à 2003. À mon avis, le rôle de juge et celui de commissaire du CST se rejoignent à plusieurs égards. En effet, un juge a pour souci premier de veiller à la tenue de procès équitables et de protéger les libertés individuelles, tout en préservant la paix et la sécurité. De même, la préoccupation fondamentale du commissaire du CST est de trouver un juste équilibre entre le droit à la protection des renseignements personnels et la nécessité d'obtenir des renseignements pour protéger la sécurité nationale. La loi reflète cette parenté de vocation en exigeant que le commissaire nommé à ce poste soit un juge surnuméraire ou un juge à la retraite d'une instance supérieure.

La préoccupation fondamentale du commissaire du CST est de trouver un juste équilibre entre le droit à la protection des renseignements personnels et la nécessité d'obtenir des renseignements pour protéger la sécurité nationale.

Dans les faits, toutefois, il existe une différence importante. Même si la question du secret se pose pour certaines actions en justice, le processus judiciaire est dans l'ensemble du domaine public. En revanche, le secret est au cœur même de la collecte des renseignements étrangers. Les principes d'équilibre sont néanmoins les mêmes. Je conçois le rôle de mon bureau comme étant de fournir à la population canadienne l'assurance que les activités cruciales du CST en matière de renseignement sont examinées avec soin par une autorité impartiale qui en vérifie la légalité et que ses droits sont protégés, sans compromettre le secret nécessaire à la protection de la sécurité nationale.

Au mois d'octobre 2006, j'ai eu l'occasion exceptionnelle de participer à la conférence internationale des organismes de surveillance du renseignement qui s'est déroulée au Cap, en Afrique du Sud. L'un des thèmes de la conférence portait sur le besoin de trouver un équilibre entre la protection des droits et libertés traditionnels des citoyens et la nécessité d'accroître les pouvoirs des autorités pour contrer les menaces à la sécurité nationale. Le fait de pouvoir

rencontrer des spécialistes de la surveillance des activités de renseignement et de sécurité en provenance de 14 pays, dont le nôtre, et de discuter avec eux des défis communs que nous avons à relever a été une expérience remarquable. Je suis très heureux d'avoir pu participer à cette conférence, car cela m'a permis, à titre de nouveau commissaire du CST, de m'imprégner de sujets d'intérêt mutuel en compagnie d'experts.

Dans les jours qui ont suivi ma nomination, j'ai rencontré le ministre de la Défense nationale et le chef du CST. J'ai en outre participé à de nombreuses séances d'information et visites, dont plusieurs au CST, et je tiens à remercier les responsables de leurs présentations détaillées. J'ai eu par la suite l'occasion de rencontrer d'autres hauts responsables du gouvernement fédéral, notamment la vérificatrice générale du Canada, la commissaire à la protection de la vie privée, les présidents du Comité de surveillance des activités de renseignement de sécurité (CSARS) et de la Commission des plaintes du public contre la GRC, ainsi que le sous-ministre et l'ombudsman de la Défense nationale.

Mais le plus important est le temps que j'ai consacré au travail de mon bureau et à me familiariser avec les activités et les préoccupations de mes prédécesseurs, ce dont je parlerai plus loin.

CONTEXTE DE L'EXAMEN

Plusieurs éléments clés ont contribué à façonner le contexte dans lequel le bureau a effectué son travail au cours de l'année écoulée. Certains de ces éléments ont été décrits et commentés par mes prédécesseurs dans leurs rapports annuels. Dans le présent rapport, j'attirerai l'attention sur des éléments qui n'ont pas été abordés jusqu'à présent, ainsi que sur des faits nouveaux survenus dans les dossiers courants.

Interprétation juridique

Depuis l'adoption de la *Loi antiterroriste* en décembre 2001, les personnes qui ont occupé le poste de commissaire du CST sont aux prises avec un dilemme persistant qui découle des modifications que cette loi omnibus a apportées à la *Loi sur la défense nationale*. La fonction d'examen du commissaire relative aux activités du CST menées sous le régime d'une autorisation ministérielle délivrée dans le seul but de recueillir des

renseignements étrangers, a été une question particulièrement épineuse, étant donné l'absence de consensus sur l'interprétation de dispositions clés de la *Loi*.

D'un côté, mes prédécesseurs et moi avons reconnu l'importance des activités du CST, ainsi que les avantages que le gouvernement du Canada retire des renseignements étrangers qu'il lui fournit, notamment à une époque où la menace du terrorisme mondial n'a pas perdu de son intensité et où la sécurité de nos soldats en Afghanistan est toujours menacée.

De l'autre, nous avons soutenu sans équivoque, pendant nos mandats respectifs, que l'interprétation et les avis juridiques concernant les autorisations ministérielles fournis au CST par le ministère de la Justice ne sauraient s'appuyer sur une simple lecture des dispositions pertinentes de la partie V.1 de la *Loi sur la défense nationale*, et chacun d'entre nous en a informé le ministre de la Défense nationale en poste. De plus, mon prédécesseur immédiat, le très honorable Antonio Lamer, et moi-même avons tous les deux fait connaître nos positions aux personnes concernées au bureau du procureur général du Canada.

Au moment de déterminer si une activité est légale, je vérifie d'abord ce que la loi dit à ce sujet. La loi pertinente devient alors l'aune à laquelle on juge de la légalité de l'activité en cause. Il est difficile de le faire lorsque, dans des cas comme celui-ci, il existe des divergences d'opinion fondamentales sur ce que dit la loi.

Je ne mets pas en doute le rôle du ministère de la Justice dans l'élaboration de la loi et je ne vois pas non plus mon rôle de commissaire comme celui d'un arbitre dans son interprétation. Toutefois, comme je l'ai mentionné au ministre de la Défense nationale et au procureur général du Canada, la loi manque de clarté et elle doit être modifiée. C'est là un point de vue que partageaient également mes deux prédécesseurs.

La loi manque de clarté et elle doit être modifiée.

Cette question est à l'étude depuis un certain temps, et j'espère que le gouvernement procédera aux modifications requises à la première occasion. Je suis convaincu que la tâche ne sera pas trop lourde, car d'autres pays ont réussi à adopter et appliquent aujourd'hui des lois pour répondre à des exigences similaires.

Retard des lois sur les progrès technologiques

Au fil du temps, le fossé ne cesse de se creuser entre les nouvelles technologies et les connaissances du grand public dans ce domaine. À plusieurs égards, les lois canadiennes n'ont pas non plus suivi le rythme de l'évolution technologique. Nous avons besoin d'une approche plus créative. À l'heure actuelle, des criminels et des terroristes sont passés maîtres de ces technologies complexes, car, contrairement aux institutions démocratiques, leur élan n'est pas freiné par des contraintes juridiques. Ceux qui participent au processus législatif doivent donc éviter de produire des lois visant les technologies du jour, qui seront vite dépassées. Nous devons plutôt veiller à ce que nos lois aient une portée assez large et soient structurées – par la réglementation ou autrement – de façon à pouvoir s'appliquer aux nouvelles technologies et ainsi à continuer de protéger à la fois notre vie privée et notre sécurité.

Examen triennal de la *Loi antiterroriste*

La *Loi antiterroriste* a modifié entre autres la *Loi sur les secrets officiels* et la *Loi sur la défense nationale*. Les modifications apportées à cette dernière comportent notamment l'établissement d'un cadre législatif pour le CST et le commissaire du CST.

La *Loi antiterroriste* prévoyait la tenue d'un examen de ses dispositions et de son application trois ans après sa sanction royale, examen qui devait être mené par un comité du Sénat ou de la Chambre des communes, ou un comité mixte, désigné ou mis sur pied à cette fin. Le Comité permanent de la sécurité publique et nationale de la Chambre a mis sur pied un sous-comité dans ce but à l'automne 2004. Parallèlement, le Sénat a également créé un comité spécial chargé de procéder à un examen approfondi de la *Loi*. Comme le mentionne le *Rapport annuel* 2005-2006, mon prédécesseur a comparu devant le Comité sénatorial spécial le 13 juin 2005 et, deux jours plus tard, devant le Sous-comité de la Chambre des communes. Le Comité sénatorial spécial a déposé son rapport le 22 février 2007, et le Sous-comité de la Chambre, le 27 mars 2007.

Recommandations du Comité sénatorial spécial

Le Comité sénatorial spécial a présenté plusieurs recommandations concernant le CST, ainsi que le bureau du commissaire. En ce qui a trait au CST, le Comité s'est concentré sur les autorisations ministérielles et s'est dit d'accord avec les explications du CST quant aux raisons pour lesquelles l'organisme a besoin d'intercepter des communications privées dans le cadre de ses activités de collecte de renseignements étrangers et de protection de la sécurité des technologies de l'information. Il a également accepté les explications du commissaire Lamer quant à la légitimité du recours à des autorisations ministérielles plutôt qu'à des autorisations judiciaires pour permettre l'interception de communications privées, étant donné que les mandats des tribunaux canadiens n'ont aucune portée à l'extérieur du pays[1]. Le Comité était rassuré par le fait que notre bureau est tenu de vérifier la légalité des activités du CST, notamment l'interception de communications privées sous le régime d'une autorisation ministérielle. Il demeurait cependant préoccupé, tout comme le commissaire Lamer, par le manque de clarté de la norme requise pour convaincre le ministre que toutes les conditions nécessaires pour recourir à l'interception de communications privées étaient remplies. Le Comité a donc recommandé que les paragraphes 273.65(2) et (4) de la *Loi sur la défense nationale* soient modifiés de façon à préciser si ces conditions doivent être fondées sur une croyance raisonnable ou sur des soupçons raisonnables[2]. Il s'agit d'une question à laquelle mon bureau attache de l'importance et une clarification serait la bienvenue.

Le Comité était rassuré par le fait que notre bureau est tenu de vérifier la légalité des activités du CST.

Comme le Comité souhaitait s'assurer que l'information interceptée était détruite s'il se révélait qu'elle n'était pas essentielle, ou lorsqu'elle n'était plus essentielle, il a recommandé que le CST élabore des politiques relatives à la conservation et à la destruction des renseignements, prévoyant notamment des délais précis pour l'élimination des renseignements interceptés, et qu'il rende ces politiques publiques[3].

---

[1] Comité sénatorial spécial sur la *Loi antiterroriste*, *Justice fondamentale dans des temps exceptionnels : Rapport principal du Comité sénatorial spécial sur la* Loi antiterroriste, février 2007, p. 83.
[2] *Ibid.*, recommandation n° 18, p. 85.
[3] *Ibid.*, recommandation n° 19, p. 85.

Dans le but de satisfaire aux principes de la reddition de comptes et de la transparence, le Comité a en outre recommandé que le ministre de la Défense nationale ou le CST soit tenu de rendre compte annuellement au Parlement du nombre d'autorisations ministérielles accordées au cours de l'année, du nombre d'autorisations encore en vigueur à la fin de l'année et du but général pour lequel chacune d'elles a été accordée (c'est-à-dire, pour l'obtention de renseignements étrangers ou pour la protection des systèmes ou réseaux informatiques)[4].

La *Loi antiterroriste* a également modifié la *Loi sur les secrets officiels* et l'a rebaptisée *Loi sur la protection de l'information*. Cette loi établit le processus que les personnes astreintes au secret à perpétuité doivent suivre pour se prévaloir de la défense d'intérêt public en vue de la divulgation de renseignements classifiés. Le commissaire peut recevoir des renseignements classifiés dans le cadre de ce processus (voir l'annexe A). Or, la *Loi sur la protection de l'information* ne précise pas ce qu'il doit faire lorsque ces renseignements sont entre ses mains[5]. Le Comité a recommandé que le gouvernement précise la marche à suivre dans ce cas[6]. Je dois mentionner que mon bureau s'est doté de politiques et de procédures internes pour combler les lacunes cernées par le Comité.

Enfin, le Comité a discuté de la surveillance et de l'examen des dispositifs canadiens en matière de sécurité nationale et de lutte contre le terrorisme. Il a mentionné que notre bureau « est généralement perçu comme étant un mécanisme de surveillance efficace »[7]. Il a recommandé qu'un comité sénatorial permanent soit mis sur pied pour surveiller la législation antiterroriste et les dispositifs de sécurité nationale et qu'il rende compte périodiquement de ses conclusions. Le Comité a en outre recommandé que le Parlement procède à un examen approfondi des dispositions et de l'application de la *Loi antiterroriste* tous les cinq ans.

---

[4] *Ibid.*, recommandation n° 20, p. 86.
[5] À ce jour, je n'ai reçu aucun renseignement en vertu de la *Loi sur la protection de l'information*.
[6] *Supra*, note 1, recommandation n° 26, p. 103.
[7] *Supra*, note 1, p. 128.

Recommandations du Sous-comité de la Chambre des communes

Dans son rapport final sur l'examen de la *Loi antiterroriste*, le Sous-comité de la Chambre a également traité de la question des autorisations ministérielles. J'ai été heureux de constater en particulier que le Sous-comité a mis en relief les observations de mon prédécesseur dans son rapport annuel 2005-2006 au sujet des ambiguïtés et imprécisions des dispositions de la loi à ce sujet, et des divergences entre mon bureau et le ministère de la Justice sur l'interprétation de ces dispositions. Sans formuler de recommandation particulière à ce sujet, le Sous-comité nous a néanmoins pressés, le conseiller juridique du gouvernement et moi-même, de régler cette question dans les meilleurs délais. Il a de plus demandé que le gouvernement précise, dans sa réponse au rapport final du Sous-comité et dans la mesure du possible, les points de désaccord et la façon dont ils ont été réglés. Si cela n'est pas fait, le Sous-comité est d'avis que je devrais fournir ces renseignements dans mon rapport annuel 2007-2008[8]. J'entends réexaminer cette recommandation quand viendra le temps de préparer ce rapport.

La méthode d'examen de mon bureau prévoit toujours un examen de conformité à la Charte *et à la* Loi sur la protection des renseignements personnels.

Le Sous-comité a également fait sienne la recommandation de la commissaire à la protection de la vie privée voulant que le paragraphe 273.65(8) de la *Loi sur la défense nationale* soit modifié de manière à ce que le commissaire du CST soit tenu d'examiner les activités d'interception de communications privées découlant d'une autorisation ministérielle, afin de s'assurer qu'elles respectent les exigences de la *Charte canadienne des droits et libertés* et de la *Loi sur la protection des renseignements personnels*, de même que l'autorisation elle-même. Cette position a été appuyée par une autre recommandation voulant que l'article 273.66 de la *Loi sur la défense nationale* soit modifié de manière à ce que le CST ne puisse entreprendre que des activités qui sont compatibles avec la *Charte canadienne des droits et libertés* et la *Loi sur la protection des renseignements personnels*, ainsi qu'avec les restrictions à l'exercice de son mandat déjà établies dans cet article[9].

---

[8] Sous-comité sur la revue de la *Loi antiterroriste*, *Droits, restrictions et sécurité : un examen complet de la* Loi antiterroriste *et des questions connexes*, *Rapport final du Comité permanent de la sécurité publique et nationale*, mars 2007, p. 64.

[9] *Ibid.*, recommandations nos 44 et 45, pp. 63-64.

Je dois souligner que la méthode d'examen de mon bureau prévoit toujours un examen de conformité à la *Charte* et à la *Loi sur la protection des renseignements personnels*.

Quant à l'examen et à la surveillance, le Sous-comité a recommandé que le projet de loi C-81 déposé pendant la 38e législature, *Loi sur le Comité de parlementaires sur la sécurité nationale*, ou une variante de celui-ci, soit déposé au Parlement à la première occasion. En outre, il a recommandé que le mandat de ce comité comprenne des vérifications de la conformité de certains ministères et organismes, tels que le Service canadien du renseignement de sécurité (SCRS) et le CST, et des éléments de la GRC chargés de la sécurité nationale, avec les dispositions de la *Loi antiterroriste*[10]. Dans son rapport annuel de l'an dernier, mon prédécesseur appuyait l'idée d'un examen parlementaire plus dynamique des activités liées à la sécurité nationale, mais soulignait également les défis qui y sont associés, notamment en ce qui a trait à la composition du comité et à son accès à des documents et renseignements classifiés. Je souscris à cette position dans l'ensemble et je me propose de présenter des observations précises sur le sujet lorsqu'un projet de loi sera déposé.

Enfin, le Sous-comité a recommandé qu'on procède à un autre examen complet des dispositions et de l'application de la *Loi antiterroriste* devant commencer au plus tard le 31 décembre 2010 et se terminer au plus tard le 31 décembre 2011. Il a souligné que le comité de parlementaires proposé serait bien placé pour procéder à cet examen[11].

Commission d'enquête O'Connor

La Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar a été mise sur pied le 5 février 2004. Elle a reçu le mandat d'enquêter et de faire rapport sur les actions des responsables canadiens relativement à Maher Arar (enquête sur les faits), ainsi que de formuler des recommandations sur la création d'un mécanisme d'examen indépendant des activités de la GRC liées à la sécurité nationale (examen de la politique). L'honorable Dennis O'Connor a été nommé commissaire de l'enquête. Il a publié son rapport sur l'examen de la politique le 12 décembre 2006.

---

[10] *Ibid.*, recommandations nos 58 et 59, pp. 94-96.
[11] *Ibid.*, pp. 93-95.

Pour pouvoir procéder à un examen intégré des activités de sécurité nationales intégrées, le commissaire O'Connor a recommandé que des passerelles législatives soient établies entre la Commission indépendante d'examen des plaintes et des activités en matière de sécurité nationale visant la GRC qu'il propose de créer, le Comité de surveillance des activités de renseignement de sécurité et le Bureau du commissaire du CST afin de permettre l'échange d'information, le renvoi d'enquêtes à un autre organisme, la tenue d'enquêtes conjointes, ainsi que la coordination et la préparation des rapports[12]. Je suis favorable à cette proposition, bien qu'à ce jour l'absence de passerelle n'ait jamais été un obstacle opérationnel.

J'ai pris note avec satisfaction de l'observation suivante dans le rapport du juge O'Connor : « Je ne recommande pas d'élargir le mandat du CSARS au CST car je crois comprendre que le Bureau du commissaire du CST fonctionne très bien. Je ne vois donc aucune raison d'intervenir dans ses activités. »[13] J'ai également été heureux de constater que mon bureau avait été félicité pour la création en 2005-2006 de la Tribune des organismes d'examen[14]. Je reviendrai sur cette dernière un peu plus loin.

J'ai quelques réserves toutefois à propos de la recommandation du juge O'Connor de créer un comité de coordination pour l'examen intégré des questions de sécurité nationale[15]. Je crains en effet que la création d'un tel comité par voie législative – et la modification des lois connexes – n'introduise un niveau de bureaucratie superflu et improductif entre les organismes d'examen indépendants et le Parlement.

---

[12] Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar, *Un nouveau mécanisme d'examen des activités de la GRC en matière de sécurité nationale* (Ottawa : Travaux publics et Services gouvernementaux Canada, 2006), p. 643.

[13] *Ibid.*, recommandation n° 11, p. 641.

[14] *Ibid.*, p. 316.

[15] *Ibid.*, recommandation n° 12, p. 654.

RÉTROSPECTIVE DE L'ANNÉE

Examens indépendants du Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST)

Au printemps 2006, deux examens indépendants portant sur la gestion de mon bureau ont été commandés. L'un portait sur l'administration, notamment la gestion et le contrôle des ressources financières, humaines et d'information, l'autre, sur les opérations. Dans ce dernier cas, il s'agissait d'évaluer si le bureau s'acquittait bien et efficacement des responsabilités confiées au commissaire dans le cadre de son mandat.

J'ai été heureux de constater que les conclusions de ces examens administratifs étaient toutes positives.

Les rapports de ces deux examens m'ont été remis au moment de ma nomination, ce qui m'a permis de profiter d'une évaluation indépendante de mon nouveau domaine de responsabilité. J'ai été heureux de constater que les conclusions de ces examens administratifs étaient toutes positives. Les recommandations issues de l'examen opérationnel ont fait l'objet d'une discussion approfondie lors d'un atelier qui a eu lieu le 21 août 2006 et qui était animé par les consultants responsables de l'examen. Des questions de méthodologie concernant l'examen opérationnel ont été soulevées, qui seront brièvement discutées plus loin dans ce rapport.

Plan de travail

Un plan de travail triennal, mis à jour régulièrement, guide les activités de mon bureau. Pour faciliter l'établissement du calendrier, mon personnel consulte le CST sur les composantes d'examen du plan. Voici quelques exemples de critères qui déterminent leur choix des domaines qui seront soumis à un examen : les activités ou programmes du CST qui n'ont pas fait l'objet d'un examen par le passé ou récemment; les domaines recensés dans les breffages demandés au CST; la suite donnée aux recommandations issues des examens précédents; et les activités où les menaces à la vie privée sont jugées les plus élevées. Les membres de mon personnel, qui possèdent une connaissance détaillée des activités du CST, se posent des questions fondamentales comme les suivantes : qu'est-ce qui peut mal tourner? Quelles sont les probabilités que cela se concrétise? Le cas échéant, quelles seraient les répercussions?

De plus, au cours de l'année, nous avons consacré beaucoup de temps et de ressources aux questions liées à l'interprétation des textes de loi, dont j'ai parlé en détail dans la section portant sur le contexte de l'examen.

Examens effectués

Mon mandat d'examen général est défini à l'alinéa 273.63(2)*a*) de la *Loi sur la défense nationale*[16]. De plus, en vertu du paragraphe 273.65(8) de la *Loi*, je suis tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation ministérielle pour en contrôler la conformité, et de rendre compte du résultat de mon enquête au ministre.

Les autorisations ministérielles visant la collecte de renseignements étrangers sont accordées en vertu du paragraphe 273.65(1) de la *Loi sur la défense nationale*, tandis que les autorisations ministérielles visant les activités axées sur la sécurité des technologies de l'information sont accordées en vertu du paragraphe 273.65(3) de la *Loi*. Le BCCST procède à l'examen des activités du CST exercées sous le régime d'une autorisation ministérielle uniquement après que celle-ci est venue à échéance.

Pendant l'année 2006-2007, mon bureau a présenté au ministre quatre rapports d'examen classifiés, dont deux portaient sur les activités du CST exercées sous le régime d'une autorisation ministérielle – l'un sur la collecte des renseignements étrangers et l'autre sur la sécurité des technologies de l'information. Les deux autres examens ont été menés en vertu de mon mandat général, afin de contrôler la légalité des activités du CST.

[16] Les sections pertinentes de la *Loi sur la défense nationale* sont reproduites à l'annexe A.

POINTS SAILLANTS EN 2006-2007

Examen des activités de collecte de renseignements étrangers effectuées par le CST à l'appui des activités de la GRC

Contexte

En janvier 2005, mon bureau a présenté un rapport au ministre de la Défense nationale sur les résultats de son examen des activités d'assistance technique et opérationnelle fournies par le CST à la GRC en vertu de l'alinéa 273.64(1)*c*) de la *Loi sur la défense nationale*, communément appelé partie c) du mandat du CST[17]. Après la deuxième et dernière phase de l'examen, mon prédécesseur a présenté, en juin 2006, un rapport de suivi sur l'examen des activités de collecte de renseignements électromagnétiques étrangers effectuées par le CST à l'appui de la GRC, en vertu de l'alinéa 273.64(1)*a*) de la *Loi sur la défense nationale*, ou partie a) de son mandat. On trouvera plus de détails sur la première phase de l'examen dans le *Rapport annuel* 2004-2005 de mon bureau.

En vertu de la partie a) de son mandat, le CST fournit deux types de renseignements étrangers à ses clients du gouvernement, notamment la GRC. La plupart de ses rapports portent sur des domaines d'intérêt général qui aident le client à s'acquitter des fonctions de son propre mandat. En plus de fournir ce type de soutien proactif, le CST offre un soutien réactif en répondant à des demandes de renseignements particulières que lui présentent ses clients.

Méthodologie

Le BCCST a examiné les activités du CST menées en vertu de la partie a) de son mandat pour appuyer la GRC pendant la période du 1er janvier au 31 décembre 2003. Il a reçu des réponses aux questions soumises tant verbalement que par écrit aux responsables du CST, ainsi que des breffages. Il a également reçu une liste des demandes de renseignements présentées au CST par la GRC et en a examiné plusieurs de manière approfondie. Lors de cet examen, les responsables du BCCST ont reçu deux démonstrations distinctes des activités à l'étude par le personnel du CST chargé directement des demandes.

[17] Le mandat du CST est défini à l'annexe E.

Conclusions

Nombre de conclusions et recommandations contenues dans le premier rapport de mon bureau s'appliquent également à la deuxième phase de l'examen des activités d'assistance fournies en vertu de la partie a) du mandat du CST, notamment la recommandation qui lui a été faite de modifier ou de mettre à jour les instruments sur lesquels s'appuie le soutien qu'il offre à la GRC. Mon prédécesseur était heureux d'annoncer que le CST avait accepté la plupart de ces recommandations et qu'il s'employait à les mettre en œuvre.

Le CST a indiqué qu'il accordait une très haute importance à l'élaboration et à la mise en place d'un système de gestion des dossiers.

Le CST a, par ailleurs, reconnu la nécessité de mettre en place un système officiel de tenue des dossiers. Cet aspect demeure une source de préoccupation, comme le mentionne le *Rapport annuel* 2005-2006 de mon bureau. Le CST a indiqué qu'il accordait une très haute importance à l'élaboration et à la mise en place d'un système de gestion des dossiers électroniques et imprimés répondant à ses besoins.

Pendant la deuxième phase de l'examen, une vérification approfondie de la réponse du CST aux demandes de renseignements de la GRC a fait ressortir deux sources de préoccupation exigeant un examen juridique plus approfondi de la part du CST. La première était de savoir si les demandes de renseignements de la GRC dans le cadre de ses enquêtes criminelles au pays relèvent de la partie a) du mandat du CST. En attendant que le CST réexamine la question, la légalité de ses activités d'assistance à cet organisme en vertu de la partie a) de son mandat tel qu'il est actuellement interprété et appliqué par le CST n'a pas été évaluée. Le personnel de mon bureau suit le dossier.

La deuxième source de préoccupation concernait les politiques et pratiques du CST en matière de divulgation de renseignements personnels sur des Canadiens à ses clients. Lorsqu'il recueille des renseignements étrangers, le CST peut incidemment acquérir des renseignements personnels sur des Canadiens. Il peut conserver ces renseignements s'il les juge indispensables à la compréhension des renseignements étrangers et les inclure dans ses rapports sur le renseignement étranger pour autant qu'ils soient supprimés,

c'est-à-dire remplacés par une référence générique telle que « un Canadien ». Par la suite, quand il reçoit une demande de divulgation de renseignements personnels sur des Canadiens, le CST exige de son client, y compris la GRC, qu'il justifie son droit d'obtenir cette information en vertu de son propre mandat et qu'il fournisse une justification opérationnelle de son besoin de connaître ces renseignements. Si ces conditions sont réunies, le CST divulgue l'information.

Un examen approfondi des articles pertinents de la *Loi sur la défense nationale* et de la *Loi sur la protection des renseignements personnels* a soulevé la question du respect, par le CST, des diverses autorisations régissant la divulgation. C'est pourquoi mon bureau a recommandé que le CST réexamine aussi ses pouvoirs en matière de collecte, d'utilisation et de divulgation de renseignements personnels à certains ministères et organismes fédéraux. De plus, il a recommandé que le CST conclue des ententes avec ses clients, afin d'officialiser les situations dans lesquelles il peut divulguer ces renseignements lorsqu'il fournit une assistance en vertu de la partie c) de son mandat.

Le CST a reconnu que le rapport soulevait diverses questions qui, d'un point de vue stratégique/juridique, nécessiteront une analyse approfondie de la part du CST et du conseiller juridique du ministère de la Justice. Je prévois que cette analyse comprendra une étude et peut-être même une prise de position officielle et claire de la part du CST sur l'application de la *Loi sur la défense nationale* en ce qui a trait à la prestation de renseignements étrangers en conformité avec les priorités du gouvernement du Canada en matière de renseignement.

Examen des activités liées à la protection de la sécurité des technologies de l'information au sein d'un ministère

Contexte

L'examen a porté sur les activités liées à la protection de la sécurité des technologies de l'information exercées par le CST sous le régime d'une autorisation ministérielle en 2004-2005 au sein d'un ministère. L'objectif était d'évaluer et de vérifier si ces activités étaient conformes à la loi et respectaient les dispositions de l'autorisation ministérielle.

Les personnes qui communiquent avec le gouvernement pour des raisons personnelles ou d'affaires ont des attentes raisonnables touchant la protection de leur vie privée. Toutefois, en effectuant des tests pour vérifier si les réseaux et les systèmes d'informatique du gouvernement sont bien protégés, il arrive parfois que des communications privées ou des renseignements personnels soient interceptés par inadvertance. Le paragraphe 273.65(3) de la *Loi sur la défense nationale* prévoit ce qui suit :

Les personnes qui communiquent avec le gouvernement pour des raisons personnelles ou d'affaires ont des attentes raisonnables touchant la protection de leur vie privée.

> Le ministre peut, dans le seul but de protéger les systèmes ou les réseaux informatiques du gouvernement du Canada de tout méfait ou de toute utilisation non autorisée ou de toute perturbation de leur fonctionnement, autoriser par écrit le Centre de la sécurité des télécommunications à intercepter, dans les cas visés à l'alinéa 184(2)c) du *Code criminel*, des communications privées qui sont liées à une activité ou une catégorie d'activités qu'il mentionne expressément.

Dans ce cas, le CST a la responsabilité de demander une autorisation au nom du ministère ou de l'organisme pour demander que l'activité soit couverte. L'autorisation ministérielle permet au CST de procéder à une évaluation complète des réseaux et systèmes informatiques d'un ministère.

Méthodologie

L'examen a consisté dans un premier temps à examiner les documents et dossiers liés à l'autorisation ministérielle et les conditions imposées par cette dernière. On a ensuite procédé à des entrevues d'enquête et de vérification avec le CST et les représentants de certains clients qui avaient participé directement au processus d'autorisation ou aux activités qui ont suivi.

Conclusions

Sous la réserve ci-dessous au sujet d'une des conditions prévues dans l'autorisation ministérielle, l'examen a révélé que les activités du CST effectuées au sein du ministère étaient conformes à la loi et respectaient les dispositions de l'autorisation ministérielle.

L'examen a révélé que le processus d'acquisition par le CST de l'autorisation ministérielle nécessaire pour mener ses activités au sein du ministère était conforme aux exigences de la *Loi sur la défense nationale*. L'examen a en outre révélé que quatre des cinq conditions prévues au paragraphe 273.65(4) de la *Loi* étaient remplies. En ce qui concerne l'une d'entre elles toutefois, l'examen a fait ressortir que certains renseignements ont été conservés, même si leur conservation n'était pas essentielle. Bien que le personnel du CST ait agi conformément aux directives reçues, certains éléments pourraient être améliorés, et le CST a entrepris de le faire. Le CST a en outre indiqué que les prochains protocoles d'entente qui seront conclus avec ses ministères clients concernant des activités liées à la protection de la sécurité des technologies de l'information qui sont menées sous le régime d'une autorisation ministérielle rendront compte de ces améliorations.

Les autres recommandations issues de l'examen sont, entre autres, de veiller à ce que les pratiques et politiques du CST touchant les tâches confiées à son personnel au cours des activités menées dans le but de protéger la sécurité des technologies de l'information favorisent la conformité avec les pouvoirs que la loi confère au CST.

Examen des rôles des agents des relations avec la clientèle et de la Section des politiques opérationnelles du CST dans la divulgation de renseignements personnels

Contexte

L'objectif de cet examen était d'évaluer la légalité des activités à la fois des agents des relations avec la clientèle et de la Section des politiques opérationnelles du CST en ce qui a trait à la demande et à la divulgation de renseignements personnels sur des Canadiens, qui ont été supprimés des rapports du CST sur le renseignement étranger (dont nous avons parlé précédemment). L'information est mise à la disposition des clients autorisés du gouvernement du Canada à certaines conditions seulement.

Depuis sa création en 1946, le CST fournit des rapports sur le renseignement étranger basés sur des renseignements d'origine électromagnétique aux responsables concernés des ministères. Ces rapports étaient remis en main propre jusqu'à la création en 1985 du programme des agents des relations avec la clientèle sur place. Ces agents fournissent des

rapports sur le renseignement, expliquent aux clients individuels et potentiels le rôle du CST et du renseignement électromagnétique, et aident à établir les besoins des clients en fonction des priorités du gouvernement du Canada en matière de renseignement.

Pour protéger la vie privée, le CST supprime dans ses rapports sur le renseignement étranger les données personnelles qui concernent des Canadiens. Si un client a l'autorisation nécessaire et le besoin de connaître cette information, il peut l'obtenir en présentant une demande officielle accompagnée de preuves justificatives. Toutes les demandes de divulgation de renseignements sont acheminées à la Section des politiques opérationnelles du CST.

Pour protéger la vie privée, le CST supprime dans ses rapports sur le renseignement étranger les données personnelles qui concernent des Canadiens.

La majorité des demandes est maintenant acheminée directement au CST par l'entremise d'un réseau de communication sécurisé. Les agents des relations avec la clientèle jouent un rôle dans la divulgation de ces renseignements parce qu'ils traitent les demandes des clients qui n'ont pas accès à ce réseau sécurisé.

Méthodologie

L'examen a consisté à examiner les documents pertinents, notamment les pouvoirs qui régissent les activités des agents des relations avec la clientèle et l'unité du CST autorisée à divulguer l'information. Toutes les demandes de divulgation et les divulgations comme telles de renseignements supprimés sur une période de six mois ont été passées au peigne fin pour vérifier leur conformité avec la loi et la politique. Des entrevues ont été menées avec les agents des relations avec la clientèle, leurs gestionnaires, ainsi qu'avec le gestionnaire de la Section des politiques opérationnelles.

Conclusions

L'examen a permis de conclure que les activités des agents des relations avec la clientèle et de la Section des politiques opérationnelles du CST étaient conformes à la *Loi sur la défense nationale* et aux politiques connexes du CST. Nous avons constaté toutefois quelques incohérences dans les demandes et les divulgations. Nous avons en outre constaté que la politique et la pratique pourraient être améliorées à certains égards afin de mieux protéger les renseignements personnels, comme l'exige la *Loi sur la protection des renseignements personnels*. Les recommandations à ce sujet

étaient, entre autres, de fournir une formation plus complète aux clients qui présentent des demandes et d'accorder à plus de clients un accès électronique sécurisé afin de réduire les risques d'erreur et d'améliorer le contrôle du processus. Je suis heureux de constater que depuis l'examen, le CST a en outre accru la formation et la supervision de son personnel qui travaille dans la Section des politiques opérationnelles en ce qui a trait à la divulgation des renseignements supprimés.

Examen des activités de collecte de renseignements électromagnétiques menées par le CST sous le régime d'une autorisation ministérielle

Contexte

Des activités de collecte de renseignements étrangers ont été menées sous le régime de trois autorisations ministérielles qui ont été en vigueur de mars 2004 à décembre 2006. Ces autorisations ministérielles visaient l'interception de communications utiles aux fins du renseignement étranger, sur l'infrastructure mondiale d'information[18].

Compte tenu des caractéristiques des technologies de communication modernes, le CST court le risque inhérent, lorsqu'il tente d'intercepter les communications d'entités qui se trouvent à l'étranger, d'intercepter en même temps des communications privées de Canadiens. C'est pourquoi il doit obtenir une autorisation ministérielle à cette fin. En plus des conditions prévues au paragraphe 273.65(2) de la *Loi sur la défense nationale*, la directive ministérielle stipule d'autres conditions régissant la gestion des renseignements recueillis.

Mon bureau procède à un examen en deux parties des activités menées sous le régime de ces autorisations ministérielles, suivant l'interprétation donnée de la loi par le ministère de la Justice, qui est discutée ci-après. L'objectif de la première partie était d'établir un contexte et des critères pour pouvoir procéder à un examen en profondeur de ces activités complexes. J'ai remis au ministre de la Défense nationale un rapport sommaire sur cette partie de l'examen en février 2007.

[18] « Infrastructure mondiale d'information » s'entend notamment des émissions électromagnétiques, des systèmes de communication, des systèmes et réseaux des techniques de l'information ainsi que des données et des renseignements techniques qu'ils transportent, qui s'y trouvent ou qui les concernent. (*Loi sur la défense nationale*, article 273.61)

Méthodologie

Afin de bien comprendre cette forme de collecte de renseignements étrangers et les défis particuliers qu'elle présente, la première partie de l'examen comportait : l'examen des pouvoirs conférés et des conditions imposées au CST par les autorisations ministérielles, la directive ministérielle et les dispositions connexes; l'examen des politiques et des procédures que le CST a élaborées en la matière, ainsi que du cadre de gestion qu'il a mis en place pour superviser ces activités.

Conclusions

Cette partie de l'examen nous a permis de comprendre l'historique de cette activité et sa raison d'être. Elle nous a également permis de mieux comprendre les complexités organisationnelles qui l'entourent, les autorisations qui la régissent, ainsi que les conditions imposées et les programmes en place pour mettre en œuvre les autorisations, tout en respectant les conditions qui y sont attachées. Enfin, cette partie nous a en outre permis d'établir les critères régissant la deuxième et dernière partie de l'examen, qui est en cours actuellement.

Aperçu des conclusions pour 2006-2007

Je suis à même de déclarer que, dans l'ensemble, les activités du CST examinées pendant la période de référence sont conformes à la loi, sauf dans un cas. Ce cas concerne l'une des conditions d'une autorisation ministérielle visant à vérifier la sécurité des technologies de l'information. Le CST a déjà entrepris de corriger la situation. Un rapport sur l'assistance fournie à la GRC ne contenait pas d'évaluation de la légalité des activités à l'examen, le CST devant réexaminer les questions juridiques soulevées.

Pour ce qui est des activités de collecte de renseignements électromagnétiques effectuées par le CST sous le régime d'une autorisation ministérielle, je tiens à réitérer mon désaccord sur l'interprétation donnée par le ministère de la Justice aux dispositions de la *Loi sur la défense nationale* à cet égard. J'ai accepté d'évaluer la légalité des activités du CST menées en vertu de ces autorisations en me fondant sur cette dernière interprétation en attendant que la loi soit modifiée à la première occasion comme j'en ai signalé l'urgence. Je sais gré au chef du CST de son appui à ces modifications.

Examens en cours / rapports à venir

Au cours du prochain exercice financier, je ferai rapport sur divers examens actuellement en cours qui portent notamment sur les activités du CST liées à l'antiterrorisme, son utilisation des métadonnées, son soutien au SCRS, son utilisation des technologies pour protéger la vie privée des Canadiens et ses activités touchant la collecte de renseignements étrangers et la protection de la sécurité des technologies de l'information menées sous le régime de plusieurs autorisations ministérielles. De plus, mon bureau entreprendra divers autres examens, qui seront réalisés dans le cadre de mon mandat général ou de mes fonctions découlant des dispositions sur les autorisations ministérielles.

Plaintes relatives aux activités du CST

Dans le cadre de mon mandat, je dois procéder à toute enquête que je considère nécessaire par suite d'une plainte, afin de déterminer si certaines activités du CST ont été ou sont illégales.

Au cours de l'année 2006-2007, mon bureau n'a reçu aucune plainte ayant nécessité une enquête officielle. Au printemps 2006, il a toutefois terminé une enquête relative à une plainte reçue l'année précédente. Un rapport complet détaillant les faits et les conclusions de l'enquête a été remis au ministre de la Défense nationale.

Je suis en mesure de rapporter que l'enquête n'a révélé aucune activité illégale de la part du CST.

Bien que les renseignements sur cette plainte soient classifiés, je suis en mesure de rapporter que l'enquête n'a révélé aucune activité illégale de la part du CST. Mon bureau a présenté au CST des recommandations qui ont été acceptées et qui permettront de renforcer la conformité.

Fonctions exercées en vertu de la *Loi sur la protection de l'information*

La *Loi sur la protection de l'information* m'autorise à recevoir des renseignements de personnes astreintes au secret à perpétuité qui veulent se prévaloir de la défense « d'intérêt public » concernant la divulgation de renseignements classifiés. Aucun problème de ce genre n'a été soumis à mon bureau en 2006-2007.

BUREAU DU COMMISSAIRE

Pour accomplir mon mandat, je suis secondé par un effectif de huit employés à temps plein qui possèdent une vaste expérience au sein de la collectivité de la sécurité et du renseignement. Nous avons en outre parfois recours à des spécialistes de divers domaines, notamment l'informatique, les technologies, la recherche, l'élaboration des politiques et les communications, que nous embauchons à contrat selon les besoins.

Mon bureau partage souvent les mêmes intérêts et préoccupations que d'autres organismes canadiens de surveillance de la sécurité et du renseignement. Comme l'a mentionné le juge O'Connor, les employés de mon bureau ont mis sur pied en 2005-2006 la Tribune des organismes d'examen, qui leur permet de rencontrer à intervalle régulier les employés du Comité de surveillance des activités de renseignement de sécurité, du Bureau de l'Inspecteur général du Service canadien du renseignement de sécurité et de la Commission des plaintes du public contre la GRC. En 2006-2007, les membres de la Tribune se sont réunis à deux reprises pour discuter de diverses questions, notamment des recommandations contenues dans le rapport sur l'examen de la politique du juge O'Connor, ainsi que des modifications à la *Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles* résultant de la nouvelle *Loi fédérale sur la responsabilité* (projet de loi C-2). Les membres de la Tribune ont, en outre, discuté des façons de fournir à leurs organismes respectifs des délais raisonnables pour répondre aux examens, ainsi que des différentes manières de procéder lorsque des retards se produisent.

Les employés de mon bureau ont, de plus, participé à d'autres conférences et symposiums, notamment la conférence internationale des organes de surveillance du renseignement qui a eu lieu au Cap, dont j'ai parlé précédemment, et aux conférences de l'Association canadienne pour les études de renseignement et de sécurité (ACERS) et de l'Association du Barreau de l'Ontario. De plus, mon bureau a accueilli deux étudiants prometteurs à la conférence de l'ACERS pour leur offrir une occasion de perfectionnement.

En 2006-2007, mon site Web a reçu quelque 96 000 visites.

Bien que mon bureau n'ait pas de mandat éducatif officiel, je crois qu'il est important que les Canadiens sachent ce que fait le BCCST. Le Bureau possède donc un site Web (www.csec-cest.gc.ca), qui décrit son mandat et ses activités. Le site attire un public international au-delà du continent nord américain, notamment des visiteurs d'Europe, d'Asie et du Moyen-Orient. En 2006-2007, mon site Web a reçu quelque 96 000 visites.

En 2006-2007, les dépenses de mon bureau se sont chiffrées à 1 267 612 $, et ont été largement couvertes par le budget approuvé pour cette période. On trouvera un résumé de ces dépenses à l'annexe C.

REGARD SUR L'AVENIR

Commission d'enquête Major et Enquête interne Iacobucci

Deux nouvelles enquêtes pourraient avoir des répercussions sur le contexte des futurs examens : la Commission d'enquête relative aux mesures d'investigation prises à la suite de l'attentat à la bombe commis contre le vol 182 d'Air India, présidée par l'honorable John Major, et l'Enquête interne sur les actions des responsables canadiens relativement à Abdullah Almalki, Ahmad Abou-Elmaati et Muayyed Nureddin, présidée par l'honorable Frank Iacobucci.

La Commission sur l'affaire d'Air India a pour mandat de faire part au gouvernement de ses conclusions et recommandations sur les analyses et les actions des représentants du gouvernement canadien avant et après les attentats à la bombe de 1985, ainsi que sur les mesures à prendre pour éviter que toute erreur ne se reproduise. L'Enquête interne a pour mandat d'examiner tous les aspects de la participation des responsables canadiens relativement à la détention des trois personnes concernées en Syrie ou en Égypte.

Méthodologie de l'examen

L'une des recommandations issues de l'examen opérationnel indépendant des activités de mon bureau réalisé au printemps 2006 préconisait de documenter officiellement la méthodologie utilisée par le Bureau pour examiner les activités du CST. J'appuie sans réserve cette recommandation et je suis convaincu que le Bureau en bénéficiera tant dans l'immédiat qu'à long terme. Ce sera là une de ses préoccupations importantes au cours de l'été.

Conclusion

Au moment de prendre acte du bilan des huit derniers mois, j'aimerais exprimer ma gratitude à mon prédécesseur, le très honorable Antonio Lamer, de qui j'ai hérité d'un excellent personnel et d'une organisation bien placée pour relever les défis qui l'attendent. Grâce à cet héritage, j'ai été en mesure de m'acquitter de mes responsabilités au moment même de ma nomination, et la transition s'est fait sans heurt.

Je compte entretenir les rapports productifs qui ont été mis en place.

Je compte entretenir les rapports productifs qui ont été mis en place avec le ministre de la Défense nationale, le CST et les représentants des autres ministères et organismes du gouvernement qui font partie de la collectivité canadienne du renseignement et de la sécurité. J'attends avec impatience en particulier la tenue de discussions qui nous permettront, je l'espère, de régler les questions d'interprétation de la loi avec lesquelles le BCCST est aux prises depuis l'adoption de la partie V.1 de la *Loi sur la défense nationale*.

ANNEXE A : MANDAT DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

***Loi sur la défense nationale* – partie V.1**

273.63 (1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

(2) Le commissaire a pour mandat

a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;

c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

(7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.

[...]

273.65 (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre.

Loi sur la protection de l'information

15. (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public. [...]

(5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes : [...]

b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession : [...]

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable.

ANNEXE B : RAPPORTS CLASSIFIÉS, 1996-2007

1. Classified Report to the Minister
   – 3 mars 1997 (TRÈS SECRET)

2. Classified Report to the Minister
   – Operational policies with lawfulness implications – 6 février 1998 (SECRET)

3. Classified Report to the Minister
   – CSE's activities under *** – 5 mars 1998 (TRÈS SECRET Mot codé/ Réservé aux Canadiens)

4. Classified Report to the Minister
   – Internal investigations and complaints – 10 mars 1998 (SECRET)

5. Classified Report to the Minister
   – CSE's activities under *** – 10 décembre 1998 (TRÈS SECRET/Réservé aux Canadiens)

6. Classified Report to the Minister
   – On controlling communications security (COMSEC) material – 6 mai 1999 (TRÈS SECRET)

7. Classified Report to the Minister
   – How we test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière de collecte et de conservation de renseignements électromagnétiques, et évaluation des efforts de l'organisme pour sauvegarder la vie privée des Canadiens)
   – 14 juin 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

8. Classified Report to the Minister
   – A study of the *** collection program – 19 novembre 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

9. Classified Report to the Minister
   – On *** – 8 décembre 1999 (TRÈS SECRET/COMINT)

10. Classified Report to the Minister
    – A study of CSE's *** reporting process — an overview (Phase I)
    – 8 décembre 1999 (SECRET/Réservé aux Canadiens)

11. Classified Report to the Minister
    – A study of selection and *** — an overview – 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)

12. Classified Report to the Minister
    – CSE's operational support activities under *** — follow-up – 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)

13. Classified Report to the Minister
    – Internal investigations and complaints — follow-up – 10 mai 2000 (SECRET)

14. Classified Report to the Minister
    – On findings of an external review of CSE's ITS program – 15 juin 2000 (SECRET)

15. Classified Report to the Minister
    – CSE's policy system review – 13 septembre 2000 (TRÈS SECRET/Réservé aux Canadiens)

16. Classified Report to the Minister
    – A study of the *** reporting process — *** (Phase II) – 6 avril 2001 (SECRET/ Réservé aux Canadiens)

17. Classified Report to the Minister
    – A study of the *** reporting process — *** (Phase III) – 6 avril 2001 (SECRET/ Réservé aux Canadiens)

18. Classified Report to the Minister
    – CSE's participation *** – 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)

19. Classified Report to the Minister
    – CSE's support to ***, as authorized by *** and code-named ***
    – 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)

20. Classified Report to the Minister
    – A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – 21 août 2002 (SECRET)

21. Classified Report to the Minister
    – CSE's support to ***, as authorized by *** and code-named ***
    – 13 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

22. Classified Report to the Minister
– CSE's *** activities carried out under the *** 2002 *** Ministerial authorization – 27 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

23. Classified Report to the Minister
– Lexicon of CSE definitions – 26 mars 2003 (TRÈS SECRET)

24. Classified Report to the Minister
– CSE's activities pursuant to *** Ministerial authorizations including *** – 20 mai 2003 (SECRET)

25. Classified Report to the Minister
– CSE's support to ***, as authorized by *** and code-named *** — Part I – 6 novembre 2003 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

26. Classified Report to the Minister
– CSE's support to ***, as authorized by *** and code-named *** — Part II – 15 mars 2004 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

27. Classified Report to the Minister
– A review of CSE's activities conducted under *** Ministerial authorization – 19 mars 2004 (SECRET/Réservé aux Canadiens)

28. Classified Report to the Minister
– Internal investigations and complaints — follow-up – 25 mars 2004 (TRÈS SECRET/Réservé aux Canadiens)

29. Classified Report to the Minister
– A review of CSE's activities conducted under 2002 *** Ministerial authorization – 19 avril 2004 (SECRET/Réservé aux Canadiens)

30. Classified Report to the Minister
– Review of CSE *** operations under Ministerial authorization – 1er juin 2004 (TRÈS SECRET/COMINT)

31. Classified Report to the Minister
– CSE's support to *** – 7 janvier 2005 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

32. Classified Report to the Minister
– External review of CSE's *** activities conducted under Ministerial authorization – 28 février 2005 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

33. Classified Report to the Minister
– A study of the *** collection program – 15 mars 2005 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

34. Classified Report to the Minister
– Report on the activities of CSE's *** – 22 juin 2005 (TRÈS SECRET)

35. Classified Report to the Minister
– Interim report on CSE's *** operations conducted under Ministerial authorization – 2 mars 2006 (TRÈS SECRET/COMINT)

36. Classified Report to the Minister
– External review of CSE *** activities conducted under Ministerial authorization – 29 mars 2006 (TRÈS SECRET/Réservé aux Canadiens)

37. Classified Report to the Minister
– Review of CSE's foreign intelligence collection in support of the RCMP (Phase II) – 16 juin 2006 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

38. Classified Report to the Minister
– Review of information technology security activities at a government department under ministerial authorization – 18 décembre 2006 (TRÈS SECRET)

39. Classified Report to the Minister
– Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – 20 février 2007 (TRÈS SECRET/ COMINT/Réservé aux Canadiens)

40. Classified Report to the Minister
– Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – 31 mars 2007 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

ANNEXE C : ÉTAT DES DÉPENSES, 2006-2007

Sommaire des articles courants

Traitements et salaires	594 551 $
Transports et télécommunications	72 839
Information	14 071
Services professionnels et spéciaux	402 620
Location	140 315
Achat de services de réparation et d'entretien	4 649
Fournitures et approvisionnements	6 404
Acquisition de machine et de matériel	29 977
Autres charges	2 186
Total	**1 267 612 $**

ANNEXE D : HISTORIQUE DU BUREAU DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

Le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) a été créé le 19 juin 1996, au moment de la nomination du premier commissaire, l'honorable Claude Bisson, O.C., ancien juge en chef du Québec. M. Bisson a occupé le poste de commissaire jusqu'en juin 2003. Le très honorable Antonio Lamer, c.p., C.C., c.d., LL.D, d.u., juge en chef du Canada (à la retraite), lui a alors succédé pour un mandat de trois ans. L'honorable Charles D. Gonthier, c.r., qui a pris sa retraite de la Cour suprême du Canada en 2003, a été nommé commissaire en août 2006.

Pendant les six premières années de son mandat (de juin 1996 à décembre 2001), le commissaire a exercé ses fonctions conformément à plusieurs décrets, pris en vertu de la partie II de la *Loi sur les enquêtes*. Au cours de cette période, il a assumé une double responsabilité : examiner les activités du Centre de la sécurité des télécommunications (CST) afin de déterminer si elles étaient en conformité avec les lois du Canada, et recevoir les plaintes relatives aux activités du CST.

Dans le sillage des attentats terroristes du 11 septembre 2001, le Parlement a adopté la *Loi antiterroriste* omnibus, qui a été promulguée le 24 décembre 2001. Cette loi modifie la *Loi sur la défense nationale*, en y ajoutant la partie V.1, qui établit le cadre législatif du BCCST et du CST, et elle confie au commissaire de nouvelles responsabilités relatives à l'examen des activités que mène le CST sous le régime d'une autorisation ministérielle.

En outre, la *Loi* omnibus a remplacé la *Loi sur les secrets officiels* par la *Loi sur la protection de l'information*, laquelle attribue au commissaire des fonctions précises pour les cas où une personne astreinte au secret à perpétuité souhaiterait invoquer la défense de l'intérêt public pour justifier la divulgation de renseignements classifiés sur le CST.

En vertu de son mandat actuel, qui inscrit dans la loi le mandat initial établi en 1996 ainsi que les nouvelles responsabilités supplémentaires décrites ci-dessus, le commissaire conserve tous les pouvoirs que confère à un commissaire la partie II de la *Loi sur les enquêtes*.